ALGEBRAIC NUMBER THEORY IN THE STUDY OF DIFFERENCE SETS

ANDREJ VUKOVIĆ

Abstract. This article concerns applications of number theory to the study of difference sets, in particular to proofs of non-existence of difference sets with given parameters (v, k, λ). It is centered around Koichi Yamamoto's 1963 paper *Decomposition Fields of Difference Sets*. We begin with an introduction to the theory of difference sets, consisting of basic definitions and results. We introduce some algebraic number theory, first covering elementary ring-theoretic concepts such as ideals, which we use to prove non-existence of a $(25, 9, 3)$-difference set in an abelian group of order 25. We then review the basic notions of Galois theory and ring theory to prepare the reader for a discussion of Yamamoto's paper. The remainder of the article is spent proving the six theorems of Yamamoto's paper, as well as stating corollaries proved in that paper and a few remarks.

1. Outline

The first quarter of this review closely follows [1] to motivate the use of algebraic number theory in the study of difference sets. The second quarter describes the Galois and field theory necessary to discuss Yamamoto's 1963 paper *Decomposition Fields of Difference Sets*. The remainder of the review is dedicated to sketching the arguments of that paper.

As this article is intended for a general audience, we must introduce some basic concepts. First, there is the idea of a difference set. When speaking about general groups, we will write the group operation multiplicatively, but when speaking about specific additive groups, we will write the group operation additively.

Definition 1.1. Let G be a group and $D \subset G$ be a non-empty subset. Suppose that $|G| = v, |D| = k$, and every non-identity element of G can be written in exactly λ ways as $d_1 d_2^{-1}$ for $d_1, d_2 \in D$. We then say that D is a (v, k, λ)-*difference set* in G.

Example 1.2. $D = \{0, 1, 2, 4, 5, 8, 10\}$ is a $(15, 7, 3)$-difference set in $\mathbb{Z}_{15}$.

The main results of Yamamoto's paper are his Theorems 2, 3, 4, 5, and 6. We state these now so that the reader has something to look forward to. However, the requisite terminology will be defined later.

Theorem 1.3 (Yamamoto, Thm. 2)**.** *Suppose that there exists a (v, k, λ)-difference set D. Let $p \mid n$ be a prime and $d \mid v$ be not equal to 1. Suppose further that $(p, d) = 1$ and that the decomposition field K_p of p is real, i.e., $K \subset \mathbb{R}$. Then the exponent of the p-component of n is even.*

Theorem 1.4 (Yamamoto, Thm. 3)**.** *(i) Retain the notation of Yamamoto's second theorem. Additionally, let p^e and p^ℓ be the p-components of n and v, respectively. Then $p^{e/2} \leq (v/d)p^{-\ell}$.*

(ii) Suppose there exists a difference set with parameters (v,k,λ). Let $p \mid n = k-\lambda$ be prime, and let p^e and p^ℓ be defined as in part (i). If e is even, then $p^{e/2} \leq vp^{-\ell}$.

Theorem 1.5 (Yamamoto, Thm. 4)**.** *Let q be a prime divisor of v such that $q \equiv -1 \pmod 4$ and let q^ℓ be the q-component of v. Assume that any prime divisor p of n satisfies (i) $ord_q p \equiv 0 \pmod 2$, (ii) $ord_{q^\ell} p = \frac{1}{2}q^{\ell-1}(q-1)$, or (iii) $p = q$. If there exists a (v,k,λ)-difference set D, then the Diophantine equation*

$$4n = x^2 + qy^2, 0 \leq x, 0 \leq y \leq \frac{v}{q^\ell}, x + y \leq \frac{2v}{q^\ell}$$

has a solution.

Theorem 1.6 (Yamamoto, Thm. 5)**.** *Let q and r be distinct prime divisors of v, let q^ℓ and r^m be the q-components and r-components of v, respectively, and let $q \equiv -1 \pmod 4$, $(\varphi(q^\ell), \varphi(r^m)) = 2$, where φ is the Euler totient function. Assume that any prime divisor of n satisfies one of the following:*
(i) $ord_q p \equiv 0 \pmod 2$ and $ord_r p \equiv 0 \pmod 2, \not\equiv 0 \pmod 4$,
(ii) $ord_{q^\ell} p = \frac{1}{2}\varphi(q^\ell)$ and $ord_{r^m} p = \varphi(r^m)$,
(iii) $p = q$ and $ord_{r^m} p = \varphi(r^m)$.

If there exists a (v,k,λ)-difference set D, then there is a solution to the Diophantine equation

$$4n = x^2 + qy^2, 0 \leq x, 0 \leq y \leq \frac{2v}{q^\ell r^m}, x + y \leq \frac{4v}{q^\ell r^m}.$$

Theorem 1.7 (Yamamoto, Thm. 6)**.** *Let q and r be prime divisors of v such that $q \equiv -1 \pmod 4, r \equiv 1 \pmod 4, (q/r) = -1$, and $(\varphi(q^\ell), \varphi(r^m)) = 2$ for q^ℓ and r^m the q- and r-components of v, respectively. Assume any prime divisor p of n satisfies either*

(i) $ord_q p \equiv 0 \pmod 2$ and $ord_r p \equiv 0 \pmod 2, \not\equiv 0 \pmod 4$, or

(ii) $ord_{q^\ell} p = \varphi(q^\ell)$ and $ord_{r^m} p = \varphi(r^m)$.

Then, if there exists a (v,k,λ)-difference set D, there is a solution to the Diophantine equation

$$4n = x^2 + qry^2, 0 \leq x, 0 \leq y \leq \frac{2v}{q^\ell r^m}, x + y \leq \frac{4v}{q^\ell r^m} - 2.$$

Essentially these theorems allow us to show that difference sets with certain choices of (v,k,λ) don't exist because they don't satisfy the given Diophantine equations.

Next, let us review certain elementary ideas in the theory of difference sets which will allow us to give a simple example of the usefulness of algebraic number theory in that setting.

2. Difference Sets Review

The following result allows us to narrow down the possibilities for (v,k,λ) when searching for difference sets.

Lemma 2.1. *If D is a (v,k,λ)-difference set in G, then*

$$k(k-1) = \lambda(v-1).$$

Proof. Let $\Delta = \{d_1 d_2^{-1} | d_1, d_2 \in G, d_1 \neq d_2\}$. Then $|\Delta| = k(k-1)$ because there are k choices for d_1 and $k-1$ choices for d_2^{-1}. But we also have $|\Delta| = \lambda(v-1)$ because there are $v-1$ non-zero elements in G and each of these appears exactly λ times in Δ. □

The study of multipliers of difference sets is a basic technique in determining whether difference sets with particular parameters exist. We recall the basic definitions.

Definition 2.2. Let D be a difference set in G. An automorphism α of G is called a *multiplier* for D if $\alpha(D) = aDb$ for some $a, b \in G$. α is called a *left multiplier* if $\alpha(D) = aD$ for some $a \in G$.

Notice that if G is abelian, then any multiplier is a left multiplier.

Definition 2.3. Let G be an abelian group, $t \in \mathbb{Z}$ relatively prime to $|G|$, and D a difference set in G. Define the automorphism $\phi_t : G \to G$ by $\phi_t(a) = a^t$. We say ϕ_t is a *numerical multiplier* for D if there exists $h \in G$ such that $\phi_t(D) = hD$. Indeed, we typically call t itself a numerical multiplier in this case.

Example 2.4. Take $G = \mathbb{Z}_{13}$ and $D = \{2, 3, 5, 11\}$. Then $\phi_3(D) = 3D = \{6, 9, 2, 7\} = 4 + D$, so 3 is a numerical multiplier for D.

Numerical multipliers allow us to find difference sets because of the First and Second Multiplier Theorems. These are stated without proof in the next section. For now, we recall the definition of the integral group ring associated to a particular group G.

Definition 2.5. Given a finite (multiplicative) group G, the *integral group ring* $\mathbb{Z}G$ is the ring of formal sums $\sum_{g \in G} a_g G$ where $a_g \in \mathbb{Z}$ for all $g \in G$ and where the ring operations are the usual ones for formal sums, i.e.,

$$\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g) g,$$

$$(\sum_{f \in G} a_f f)(\sum_{g \in G} b_g g) = \sum_{h \in G} (\sum_{fg = h} a_f b_g) h.$$

We can represent a difference set $D \subset G$ by the sum $\sum_{d \in D} d \in \mathbb{Z}G$. We then have the following result, which we state without proof.

Theorem 2.6. *Let D be a (v, k, λ)-difference set in G. Represent D as a formal sum in $\mathbb{Z}G$, define $D^{(-1)} := \{d^{-1} | d \in D\}$, and represent $D^{(-1)}$ also as a formal sum. In $\mathbb{Z}G$ we then have*

$$DD^{(-1)} = n1_G + \lambda G.$$

Similarly, we define the polynomial ring, $\mathbb{Z}[G]$.

Definition 2.7. Let G be an abelian (additive) group. Define the *polynomial ring* $\mathbb{Z}[G]$ to be the ring of formal sums $\sum_{g \in G} a_g x^g$ where $a_g \in \mathbb{Z}$ for all $g \in G$. Let x be a variable, so that $x^f x^g = x^{f+g}$. Define addition and multiplication as follows:

$$\sum_{g \in G} a_g x^g + \sum_{g \in G} b_g x^g = \sum_{g \in G} (a_g + b_g) x^g,$$

$$(\sum_{f \in G} a_f x^f)(\sum_{g \in G} b_g x^g) = \sum_{h \in G} (\sum_{f+g=h} a_f b_g) x^h.$$

In this setting, the previous theorem can be restated as follows.

Corollary 2.8. *Let D be a (v, k, λ)-difference set in G, and let G be an abelian (additive) group. For any subset $S \subseteq G$, define $S(x) \in \mathbb{Z}[G]$ by $S(x) := \sum_{s \in S} x^s$. We then have*

$$D(x)D(x^{-1}) + n + \lambda G(x).$$

3. Motivation

Before we proceed, we choose a simple example to motivate the use of algebraic number theory in the study of difference sets. Some of the most important tools in the study of abelian difference sets are the first and second multiplier theorems. We recall their statements.

Theorem 3.1. *(First Multiplier Theorem). Let D be an abelian (v, k, λ)-difference set and let p be a prime such that $p \mid n$ but $p \nmid v$. If $p > \lambda$, then p is a numerical multiplier of D.*

Theorem 3.2. *(Second Multiplier Theorem). Let D be an abelian (v, k, λ)-difference set in a group G and let $m > \lambda$ be a divisor of n such that $(m, v) = 1$. Furthermore, let t be an integer such that $(t, v) = 1$ and such that for every prime p dividing m there exists a non-negative integer f with $t \equiv p^f \pmod{\exp(G)}$. Then t is a numerical multiplier for G.*

Now suppose that $n = k - \lambda$ divides v. Then the conditions of Theorem 1.1 fail to hold because there are no primes such that $p \mid n$ and $p \nmid v$, and the conditions of Theorem 1.2 fail to hold because there is no divisor m of n such that $(m, v) = 1$. So we cannot apply either of the multiplier theorems. Indeed, there is a class of Hadamard difference sets satisfying $v = 4n$ where $n = k - \lambda$, so in their case $n \mid v$. It is therefore of practical relevance that we find a way to circumvent the problem of not being able to apply the multiplier theorems.

Before we proceed to apply algebraic number theory, we should recall some basic definitions and results from that field of study.

Definition 3.3. If ω is a primitive mth root of unity, we denote by $\mathbb{Q}(\omega)$ the smallest field extension of $\mathbb{Q}$ containing ω. This is an algebraic number field because ω satisfies $x^m + 1$ and is therefore an algebraic number. This is the *mth cyclotomic field*. It contains the subring

$$\mathbb{Z}[\omega] = \{\sum_{j=0}^{m-1} a_j \omega^j | a_j \in \mathbb{Z}\},$$

which is the set of *cyclotomic integers*.

Definition 3.4. The *ring of integers* of an algebraic number field is the set of all algebraic integers lying in that number field. We recall that the ring of integers is in fact a subring of the number field. If the number field is denoted by K, we denote its ring of integers by O_K.

Theorem 3.5. *Let ω be a primitive mth root of unity. Then $\mathbb{Z}[\omega]$ is indeed the ring of integers of $\mathbb{Q}(\omega)$.*

Proof. See, for example, Proposition 10.2 on Section 1.10, page 60 of [6]. The proof works by producing an integral basis. For more information about integral bases, see Chapter 7 of [2]. □

The following theorem is often useful. It is proved as Lemma 3.2 of [7].

Theorem 3.6. *Let ω be a primitive p^sth root of unity for a prime p. If $\sum_{j=1}^{n} a_j\omega^j = 0$ for some $a_1, ..., a_n \in \mathbb{Q}$, then $a_k = a_\ell$ whenever $k \equiv \ell \pmod{p^{s-1}}$. In particular, if ω is a primitive pth root of unity, then $a_1 = a_2 = ... = a_n$.*

Next we recall some definitions about ideals.

Definition 3.7. Given a subset $I \subseteq R$ of a ring R, we say I is an *ideal* if $(I, +)$ is a subgroup of R and for every $i \in I$ and every $r \in R$, we have $ri \in I$ and $ir \in I$. We say I is *prime* if whenever $r_1, r_2 \in R$ and $r_1r_2 \in I$, either $r_1 \in I$ or $r_2 \in I$. Given ideals $I_1, I_2 \subseteq R$, then the *product ideal* I_1I_2 is given by

$$I_1I_2 := \{\sum_{j=1}^{n} a_jb_j | a_j \in I_1, b_j \in I_2, n \in \mathbb{N}\}.$$

It is easy to verify the product ideal is an ideal. Given $a \in R$, the set

$$aR = \{ar | r \in R\}$$

is called the *ideal generated by* a. If an ideal I is of the form aR for some $a \in R$, we say I is *principal*. Clearly if $a, b \in R$, then $(aR)(bR) = (ab)R$, so the product of principal ideals is principal. A short calculation shows that the concepts of ideal, product of ideals, prime ideal, and principal ideal are all preserved under ring automorphisms, meaning, for example, that if $I \subseteq R$ is a prime ideal and $f : R \to R$ is a ring homomorphism, then $f(I) \subseteq R$ is also a prime ideal.

The following theorem is Corollary 15.9 in [8].

Theorem 3.8. *Let ω be a primitive mth root of unity. If $z \in \mathbb{Z}[\omega]$ and $z\overline{z} = 1$, then $z = \pm\omega^\ell$ for some $\ell \in \mathbb{Z}$.*

The following theorem is Theorem 2 on page 180 of [9].

Theorem 3.9. *Let ω be a primitive mth root of unity. Then every ideal in $\mathbb{Z}[\omega]$ can be written uniquely as a product of prime ideals.*

Next we have another theorem from [9]. The proof of the first part is listed as Theorem 2 on page 196 there, and the second and third parts are Propositions 13.27 and 13.28, respectively, on page 197.

Theorem 3.10. *Let ω be a primitive mth root of unity and let $R = \mathbb{Z}[\omega]$. Let $p \in \mathbb{N}$ be prime. We have the following.*
(i) Suppose $p \nmid m$. Let f be the least positive integer such that $p^f \equiv 1 \pmod{m}$. Then in R we have $pR = P_1...P_n$ where the P_i are distinct prime ideals and $n = \phi(m)/f$, where ϕ is Euler's totient function.
(ii) Let $m = p$. Then $(1 - \omega)R$ is a prime ideal in R and $pR = ((1 - \omega)R)^{p-1}$.
(iii) Suppose P is a prime ideal occurring in the prime factorization of pR, which is unique by the previous theorem. If p is odd, then P has exponent greater than 1 in that factorization if and only if $p \mid m$. If $p = 2$, then P has exponent greater than 1 if and only if $4 \mid m$.

Immediately we will see some applications to the theory of difference sets. Before we proceed, let's recall a simple definition from group theory.

Definition 3.11. If G is a finite group and $g \in G$, then $|g|$, the *order* of g, is defined to be the least $n \in \mathbb{Z}_{\geq 1}$ such that $g^n = 1_G$.

We can apply these theorems as follows.

Example 3.12. Suppose $\omega = e^{2\pi i/5}$ and $R = \mathbb{Z}[\omega]$. Suppose further that $z \in R$ is such that $z\overline{z} = 36$. We let $w = z/6$. Then $u\overline{u} = 1$. To apply Theorem 3.8, we must show $u \in R$. Once we prove this, we will be able to write $u = \pm\omega^\ell$ for some $\ell \in \mathbb{Z}$, hence $z = \pm 6\omega^\ell$.
Let us now prove that $u \in R$. Notice that $|2| = |3| = 4$ in $(\mathbb{Z}_5, \times)$ and that $\phi(5) = 4$. Therefore, by Theorem 3.10 (i), $2R$ and $3R$ are prime ideals in $\mathbb{Z}[\omega]$. We calculate

$$\begin{aligned}(zR)(\overline{z}R) &= z\overline{z}R \\ &= 36R \\ &= (2R)^2(3R)^2.\end{aligned}$$

Theorem 3.9 then implies that $zR = \overline{z}R = 6R$. So $z = 6u$ for some $u \in R$, which is precisely the u we defined earlier. The proof carries through, as shown above.

Finally, let's see how we can use this to study difference sets in a certain abelian group.

Example 3.13. Let G be an abelian group of order 25. We claim that G cannot contain a $(25, 9, 3)$-difference set. By the classification of finite abelian groups, G is either isomorphic to $\mathbb{Z}_{25}$ or $\mathbb{Z}_5 \oplus \mathbb{Z}_5$. In either case, it contains a normal subgroup N of order 5. Then G/N has order 5 and is cyclic. Let $G/N = \langle aN \rangle$. Let $\omega = e^{2\pi i/5}$. By basic results of character theory, there is a character χ, i.e., a group homomorphism from G to $\mathbb{C}^\times$, such that χ has kernel N and maps a to ω.

Suppose for the sake of contradiction that $D \subset G$ is a $(25, 9, 3)$-difference set. Let $v_j := |D \cap a^j N|$; the $\{v_j\}$ are called *intersection numbers* for D with N. We can extend χ to $\tilde{\chi} : \mathbb{Z}G \to \mathbb{Z}[\omega]$ by linearity. Then, representing D as an element of $\mathbb{Z}G$, we have

$$z := \tilde{\chi}(D) = \sum_j v_j \omega^j \in \mathbb{Z}[\omega] =: R,$$

by basic character theory. We found in the previous example that $2R$ and $3R$ are prime ideals of R. We also have $z\overline{z} = n = 6$, so $(zR)(\overline{z}R) = (2R)(3R)$. But $\overline{2} = 2, \overline{3} = 3$, so $(zR)(\overline{z}R) = (2R)(3R)$ cannot hold. It follows that no $(25, 9, 3)$-difference set can exist in an abelian group.

Now that we have seen how algebraic number theory can be used to eliminate certain difference sets, we are ready to review deeper theory before beginning our review of Yamamoto's paper.

4. Algebraic Number Theory Review

We first review some field theory. [2], [6], and [9] are good references for the material covered here, although it can be found in any standard reference on Galois theory and algebraic number theory.

Definition 4.1. Suppose K is a subfield of L, i.e., $K \subseteq L$ and K satisfies the field axioms with the same operations as F. We then write that L/K is a *field extension.*

Definition 4.2. If L/K is a field extension and every element of L is the root of a non-zero polynomial with coefficients in K, $k_n x^n + k_{n-1}x^{n-1} + ... + k_1 x + k_0$, then we say that L/K is an *algebraic* field extension.

Example 4.3. The field extension $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$ is algebraic because $a+b\sqrt{3} \in \mathbb{Q}(\sqrt{3})$ is a root of the equation $(\frac{1}{b}(x-a))^2 - 3 = 0$, which has rational coefficients.

The field extension $\mathbb{R}/\mathbb{Q}$ is not algebraic because $\pi \in \mathbb{R}$ and π is a transcendental number.

Definition 4.4. The field extension L/K is *normal* if every irreducible polynomial over K either has no root in L or splits into linear factors in L. It is *separable* if for every $k \in K$, the minimal polynomial of k has non-vanishing formal derivative.

Example 4.5. Consider $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Let $\omega := e^{2\pi i/3}$. Then, over $\mathbb{C}$,

$$x^3 - 2 = (x - \sqrt[3]{2})(x - \omega\sqrt[3]{2})(x - \omega^2\sqrt[3]{2}).$$

Clearly $x^3 - 2$ is irreducible over $\mathbb{Q}$, but it splits into a linear and a quadratic factor over $\mathbb{Q}(\sqrt[3]{2})$, as $\omega\sqrt[3]{2}, \omega^2\sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2})$. It follows that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. On the other hand, $\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}$ is normal.

Example 4.6. The extension $\mathbb{F}_p(t)/\mathbb{F}_p(t^p)$ is not separable because the minimal polynomial of t over $\mathbb{F}_p(t^p)$ is $f(x) = x^p - t^p$, but $f'(x) = px^{p-1} = 0$, as $\mathbb{F}_p(t^p)$ has characteristic p.

We usually need not consider separability because of the well-known result that any characteristic zero algebraic extension is separable, as is every algebraic extension of a finite field.

We are now ready to define a Galois extension.

Definition 4.7. An algebraic field extension L/K is *Galois* if it is normal and separable.

Proposition 4.8. *Given a Galois extension L/K, the set*

$$Gal(L/K) := \{\sigma \in Aut(L) | \sigma(k) = k \ \forall k \in K\}$$

forms a group called the Galois group of L/K.

Example 4.9. The two field automorphisms of the Galois extension $\mathbb{C}/\mathbb{R}$ are the identity and the automorphism σ given by $\sigma(z) = \overline{z}$. Therefore,

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R}) \simeq \mathbb{Z}/2\mathbb{Z}.$$

The following theorem is the basis for Galois theory.

Theorem 4.10 (Fundamental Theorem of Galois Theory)**.** *Suppose L/K is a Galois extension. There is then an inclusion-reversing bijection between subgroups of $Gal(L/K)$ and intermediate fields $L \supseteq F \supseteq K$ given by*

$$H \mapsto L^H := \{x \in L | \sigma(x) = x \ \forall \sigma \in H\} \text{ and } F \mapsto Aut(L/F).$$

Let us also review the ring-theoretic aspects of algebraic number theory, continuing the study we initiated in the previous section.

Definition 4.11. A finite field extension of $\mathbb{Q}$ is known as a *number field.*

Definition 4.12. Suppose $K/\mathbb{Q}$ is an algebraic field extension. We say an element x is *integral* over K if there exists a monic polynomial $p(x)$ with integer coefficients such that $p(k) = 0$. The set of integral elements in K forms a ring, denoted O_K, called the *ring of integers* over K.

In particular, if ω is a primitive nth root of unity, then one can show that $\mathbb{Z}[\omega]$ is the ring of integers of $\mathbb{Q}(\omega)$.

The following result was Ernst Kummer's original motivation to invent ideals.

Proposition 4.13. *If K is a number field, any ideal of O_K has a unique factorization into non-zero prime ideals. In other words, every ring of integers of a number field is a so-called Dedekind domain.*

Indeed, Kummer's invention of ideals was a response to the lack of unique factorization in certain rings of cyclotomic integers. Around the same time, Kummer's contemporary, Gabriel Lamé, not knowing about this result, produced an erroneous proof of Fermat's Last Theorem that assumed unique factorization. Although the invention of ideals did not directly help us prove Fermat's Last Theorem, it did pave the way for modern algebraic number theory.

Definition 4.14. An *integral domain* is a non-trivial commutative ring such that the product of any two non-zero elements is itself non-zero.

Example 4.15. $\mathbb{Z}$ is an integral domain, but $\mathbb{Z}_{10}$ isn't since $2 \cdot 5 \equiv 0 \pmod{10}$.

Definition 4.16. Let D be an integral domain or a field. An *absolute value* is a function $|\cdot| : D \to \mathbb{R}$ that satisfies the following four properties:
(i) $|x| \geq 0$ for all $x \in D$ (non-negativity);
(ii) $|x| = 0$ if and only if $x = 0$ (positive-definiteness);
(iii) $|xy| = |x||y|$ for all $x, y \in D$ (multiplicativity); and
(iv) $|x + y| \leq |x| + |y|$ for all $x, y \in D$ (triangle inequality).

Example 4.17. The usual Euclidean absolute value, which we denote $|\cdot|_\infty$, on $\mathbb{R}$ or any subset thereof is indeed an absolute value.

Example 4.18. The *trivial* absolute value $|\cdot|_0$ on subsets of $\mathbb{R}$ is given by $|x|_0 := 0$ if $x = 0$ and $|x|_0 := 1$ otherwise.

Example 4.19. Let p be a prime. If $x \in \mathbb{Q}$ and $x \neq 0$, x can be written uniquely in the form $x = p^n \frac{a}{b}$, where $\gcd(a, b) = 1$, a and b are not divisible by p, and n is an integer. The *p-adic absolute value* on $\mathbb{Q}$ is then given by $|0|_p := 0$ and $|x|_p := p^{-n}$. It is an exercise left to reader to check that it satisfies the four properties of an absolute value.

If $0 < c < 1$, $|\cdot|$ is an absolute value on D, and $x, y \in D$, we have $|x + y|^c \leq (|x| + |y|)^c \leq |x|^c + |y|^c$, so $|\cdot|^c$ satisfies the triangle inequality. It is easy to verify that it satisfies the other three absolute value properties and is therefore an absolute value just like $|\cdot|$ is. To avoid redundancy of this sort when categorizing absolute values, we state the following definition.

Definition 4.20. Let D be an integral domain or a field. Two absolute values $|\cdot|$ and $|\cdot|^*$ on D are *equivalent* if there exists some $c > 0, c \in \mathbb{R}$ such that $|x|^* = |x|^c$ for all $x \in D$.

The following beautiful result was proved by Ostrowski in 1916.

Theorem 4.21 (Ostrowski)**.** *Every non-trivial absolute value (i.e., every absolute value other than the trivial one) on $\mathbb{Q}$ is equivalent to either the usual Euclidean absolute value, $|x|_\infty|$, or the p-adic absolute value, $|x|_p$, for some prime p.*

Completing $\mathbb{Q}$ with respect to the Euclidean absolute value $|\cdot|_\infty$ gives $\mathbb{R} =: \mathbb{Q}_\infty$. Completing $\mathbb{Q}$ with respect to a p-adic absolute value $|\cdot|_p$ gives the field $\mathbb{Q}_p$ of *p-adic numbers*.

We often speak of completing $\mathbb{Q}$ at a *finite place* to obtain $\mathbb{Q}_p$ or of completing $\mathbb{Q}$ at the *infinite place* to obtain $\mathbb{R}$. This explains the notation $\mathbb{Q}_\infty = \mathbb{R}$ and the notation $|\cdot|_\infty$ for the Euclidean absolute value.

The following notational convenience is used in the paper we will study.

Definition 4.22. The *Hilbert norm-residue symbol* is given by

$$(a,b)_r := \begin{cases} 1, & \text{if } z^2 = ax^2 + by^2 \text{ has a non-zero solution } (x,y,z) \in (\mathbb{Q}_r)^3 \\ -1, & \text{otherwise,} \end{cases}$$

where r is a prime or $r = \infty$.

Theorem 4.23. *The Hilbert symbol $(\cdot,\cdot)_r$ has the following properties:*
(i) If a is a square, then $(a,b)_r = 1$ for all b.
(ii) For all non-zero $a, b \in \mathbb{Q}_r$, $(a,b)_r = (b,a)_r$.
(iii) If $a \in \mathbb{Q}_r$ is non-zero and $a-1$ is also non-zero and in $\mathbb{Q}_r$, then $(a, 1_a)_r = 1$.
(iv) If $a, b, c \in \mathbb{Q}_r$ are non-zero, then $(a, bc) = (a,b)(a,c)$.

The waters we are wading into by stating this proposition are very deep. Indeed, property (iv) of the previous theorem requires local class field theory for its proof.

The following sequence of definitions finally leads us to combine the terminology of Galois and ring theory with that of difference sets.

Definition 4.24. Let $p \in \mathbb{Z}$ be prime. Let ω_v be a primitive vth root of unity. Let $\mathfrak{p}$ be a prime ideal divisor of (p) in $\mathbb{Q}(\omega_v)$. We define the *decomposition group*, $D_\mathfrak{p}$, of $\mathfrak{p}$ as follows:

$$D_\mathfrak{p} := \{\theta \in \mathrm{Gal}(\mathbb{Q}(\omega_v)/\mathbb{Q}) | \theta(\mathfrak{p}) = \mathfrak{p}\}.$$

Because the field extension $\mathbb{Q}(\omega_v)/\mathbb{Q}$ is abelian, one can prove that $D_\mathfrak{p}$ is the same for all $\mathfrak{p}$ dividing p, so we can denote it by D_p with no ambiguity.

Definition 4.25. Let $v = p^\ell v'$ where $(v', p) = 1$ and $\ell \in \mathbb{Z}$. It is a result in the theory of decomposition groups that D_p is generated by maps of the form $\omega_{v'} \to \omega_{v'}^p$, known as *Frobenius automorphisms*.

Definition 4.26. D_p is a subgroup of the Galois group of the extension $\mathbb{Q}(\omega_v)/\mathbb{Q}$, by the Fundamental Theorem of Galois Theory it corresponds to a subfield of that extension, which we denote K_p and call the *decomposition field* of p.

Definition 4.27. Let D be a (v,k,λ)-difference set. Let $n := k - \lambda$, which is the conventional meaning assigned to the variable n in the theory of difference sets. Then the intersection

$$\Delta := \bigcap_{p|n} K_p$$

is known as the *decomposition field* of D.

The following definitions are simply establishing standard number-theoretic terminology.

Definition 4.28. If a, m are non-zero coprime integers, then the *order* of a modulo m, denoted $\text{ord}_m(a)$, is the least positive integer z such that $a^z \equiv 1 \pmod{m}$.

Definition 4.29. If $p \in \mathbb{Z}$ is a prime and O_K is the ring of integers of a number field K, then we say p *ramifies* in K if the principal ideal (p) is divisible by the square of some non-trivial prime ideal when factored in O_K.

We can now state the following lemma, which will be useful to us in the proof of Theorem 2 in Yamamoto's paper.

Lemma 4.30. *If $p \in \mathbb{Z}$ is prime and $(n, p) = 1$, then p does not ramify in $\mathbb{Q}(\omega_n)$.*

Moreover, Yamamoto introduces the following definitions near the beginning of his paper.

Definition 4.31. Let ω_m be a primitive mth root of unity. Let $\alpha \neq 0, \alpha \in \mathbb{Z}[\omega_m]$, and let $\mathfrak{p}$ be a non-trivial prime ideal in $\mathbb{Z}[\omega_m]$. The $\mathfrak{p}$-*component* of α is defined to be the largest power of $\mathfrak{p}$ dividing (α).

If $\mathfrak{a}$ is any non-zero ideal of $\mathbb{Z}[\omega_m]$, the $\mathfrak{a}$-*component* of α is defined to be the product of the $\mathfrak{p}$-components of α for all prime ideals $\mathfrak{p}$ in the factorization of $\mathfrak{a}$.

Definition 4.32. Let $C : \mathbb{Q} \to \mathbb{Z}[\omega_m]$ be a function. We then say that C is a *number-theoretic* function.

Definition 4.33. Let C be a number-theoretic function. Let $\rho \in \mathbb{Q}$. The *difference operator* $\Delta(\rho)$ is defined by

$$\Delta(\rho)C(i) := C(i + \rho) - C(i).$$

We impose the convention that $C(\rho) := 0$ if ρ is not an integer. We also say that C has *period* n if $\Delta(n)C(i) = 0$ for all $i \in \mathbb{Q}$.

We now study Yamamoto's paper.

5. Yamamoto's Paper

This section of course closely follows the text of Yamamoto's paper [10]. The proofs are entirely his; I have just rewritten them in my own words.

The first theorem proved in Yamamoto's paper is a useful technical tool to be used later. It is a generalization of our Theorem 3.6 stated in the notation of difference operators that we have just discussed.

Theorem 5.1 (Yamamoto, Thm. 1)**.** *Let $n = p_1^{\ell_1}...p_s^{\ell_s}$ be the prime factorization of n. Let $(m, n) = 1$, C be a number-theoretic function with period n, and let $f(x) := \sum_{i=0}^{n-1} C(i)x^i$. Let $d \mid n$ and $\alpha \in \mathbb{Z}[\omega_m]$. Then, $f(\omega_n^r) \equiv 0 \pmod{\alpha}$ for all $r \mid d$ if and only if*

$$p_1^{t_1}...p_s^{t_s}\Delta(np_1^{-t_1-1})...\Delta(np_s^{-t_s-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i and all $t_1, ..., t_s$ such that $p_1^{t_1}...p_s^{t_s} \mid d$.

Proof. The $s = 0$ case follows from our Theorem 3.6. Let $s > 1$. Choose u and ℓ so that $n = p^\ell, d = p^u$. We will induct on u.

Let $u = 0$. We calculate

$$f(\omega_n) = \sum_{i=0}^{p^{\ell-1}-1} \sum_{j=0}^{p-1} C(i + p^{\ell-1}j)\omega_n^{i+p^{\ell-1}j}$$

$$= \sum_{i=0}^{p^{\ell-1}-1} \sum_{j=1}^{p-1} (C(i + p^{\ell-1}j) - C(i))\omega_n^{i+p^{\ell-1}j},$$

as $\omega_n^{p^{\ell-1}} = \omega_p$ is a primitive pth root of unity and the sum $\sum_{j=0}^{p-1} \omega_p^j$ is then zero. Now, in the sum above we have $p^{\ell-1}(p-1)$ expressions $\omega_n^{i+p^{\ell-1}j}$ for $0 \leq i < p^{\ell-1}$ and $1 \leq j < p$. These provide a $\mathbb{Z}[\omega_m]$-basis for $\mathbb{Z}[\omega_{mn}]$ because they are $\mathbb{Z}[\omega_m]$-linearly independent and of the right dimension, so we have that $f(\omega_n) \equiv 0 \pmod{\alpha}$ if and only if $C(i + p^{\ell-1}j) - C(i) \equiv 0 \pmod{\alpha}$ for all i, j. But the condition that for all i, j we have

$$C(i + p^{\ell-1}j) - C(i) \equiv 0 \pmod{\alpha}$$

is equivalent to

$$\Delta(np^{-1})C(i) \equiv 0 \pmod{\alpha}$$

for all i. This proves the result for $u = 0$.

Now assume that $s = 1$, $u > 0$, and the result holds for smaller u. We calculate

$$f(x^p) \equiv \sum_{i=0}^{p^{\ell-1}} C(i)x^{ip}$$

$$\equiv \sum_{i=1}^{p^{\ell-1}-1} (\sum_{j=0}^{p-1} C(i + p^{\ell-1}j))x^{ip} \pmod{1 - x^n}.$$

We showed earlier that $f(\omega_n) \equiv 0 \pmod{\alpha}$ if and only if $C(i) - C(i + p^{\ell-1}j) \equiv 0 \pmod{\alpha}$. We now exploit this fact by defining

$$g(x) := p \sum_{i=0}^{p^{\ell-1}-1} C(i)x^{ip}.$$

We then have $f(x^p) \equiv g(x) \pmod{\alpha, 1 - x^n}$, and the statement that $f(\omega_n^{p^t}) \equiv 0 \pmod{\alpha}$ for all $0 \leq t \leq u$ can be restated equivalently as the condition that $f(\omega_n^{p^t}) \equiv 0 \pmod{\alpha}$ and $g(\omega_n^{p^t}) \equiv 0 \pmod{\alpha}$ for all $0 \leq t \leq u - 1$. This last condition is equivalent by our induction hypothesis to the statement that $p^t\Delta(p^{\ell-t-1})C(i) \equiv 0 \pmod{\alpha}$ and $p^{t+1}\Delta(p^{\ell-t-2})C(i) \equiv 0 \pmod{\alpha}$ for all $0 \leq t \leq u - 1$. This is equivalent in turn to the condition that for all $0 \leq t \leq u$,

$$p^t\Delta(p^{\ell-t-1})C(i) \equiv 0 \pmod{\alpha}.$$

This proves the $s = 1$ case of the theorem. We can now assume that $s > 1$ and the theorem holds for smaller s. We let $n =: n_1n'$, $n_1 =: p_1^{\ell_1}$, $n' =: p_2^{\ell_2}...p_s^{\ell_s}$, $d =: d_1d'$, $d_1 =: (n_1, d)$, $d' =: (n', d)$. Given a divisor r of d, we can write it uniquely as $r =: r_1r'$ where $r_1 \mid d_1$ and $r' \mid d$.

Given i, we can choose j, k such that $i \equiv n'j + n_1 k \pmod{n}$. Then

$$f(x) \equiv \sum_{j=0}^{n_1-1} \sum_{k=0}^{n'-1} C(n'j + n_1 k) x^{n'j+n_1 k} \pmod{1-x^n}.$$

We set

$$C^*(y, j) := \sum_{k=0}^{n'-1} C(n'j + n_1 k) y^k.$$

We can thus calculate

$$\begin{aligned} f(\omega_n^r) &= \sum_{j=0}^{n_1-1} \sum_{k=0}^{n'-1} C(n'j + n_1 k) \omega_n^{n'rj} \omega_n^{n_1 rk} \\ &= \sum_{j=0}^{n_1-1} C^*(\omega_n^{n_1 r}, j). \end{aligned}$$

Let $\xi := \omega_n^{n'}$, which is a primitive n_1th root of unity, and let $\eta := \omega_n^{n_1}$, which is a primitive n'th root of unity. Then if $f(\omega_n^r) \equiv 0 \pmod{\alpha}$, we have

$$\sum_{j=0}^{n_1-1} C^*(\eta^{r'}, j) \xi^{r_1 j} \equiv 0 \pmod{\alpha}.$$

We notice that $C^*(\eta^{r'}, j) \in \mathbb{Z}[\omega_m, \eta] = \mathbb{Z}[\omega_{mn'}]$. By the $s = 1$ case we have already proved applied to $\sum_{j=0}^{n_1-1} C^*(\eta^{r'}, j) x^j$, we obtain that $f(\omega_n^r) \equiv 0 \pmod{\alpha}$ for all $r \mid d$ if and only if

$$p_1^{t_1} \Delta_j(n_1 p_1^{-t-1}) C(n'j + n_1 k) \eta^{r'k} \equiv 0 \pmod{\alpha}$$

for all t_1 and r' satisfying $p_1^{t_1} \mid d_1$ and $r' \mid d'$. The polynomial $p_1^{t_1} \sum_{k=0}^{n'-1} \Delta_j(n_1 p_1^{-t_1-1}) C(n'j + n_1 k) x^k$ has coefficients in $\mathbb{Z}[\omega_m]$, and furthermore $(m, n') = 1$ and n' has $s-1$ distinct prime divisors. So we can apply the induction hypothesis to the polynomial to obtain that the congruence above is true if and only if

$$\begin{aligned} p_1^{t_1} ... p_s^{t_s} \Delta_j(n_1 p_1^{-t_1-1}) ... \Delta_k(n' p_s^{-t_s-1}) C(n'j + n_1 k) &= p_1^{t_1} ... p_s^{t_s} \Delta(n p_1^{-t_1-1}) ... \Delta(n p_s^{-t_s-1}) C(i) \\ &\equiv 0 \pmod{\alpha} \end{aligned}$$

for all i and all $t_1, ..., t_s$ such that $p_1^{t_1} ... p_s^{t_s} \mid d$. This was what we wanted, so the theorem is proved. □

The following corollary, which we will not prove, immediately follows from Theorem 1.

Corollary 5.2. *Retain the notation of Theorem 1, and let S be a set of divisors of n such that $r \in S$ and $r' \mid r$ implies $r' \in S$. Then $f(\omega_n^r) \equiv 0 \pmod{\alpha}$ for all $r \in S$ if and only if*

$$p_1^{t_1} ... p_s^{t_s} \Delta(n p_1^{-t_1-1}) ... \Delta(n p_s^{-t_s-1}) C(i) \equiv 0 \pmod{\alpha}$$

for all i and all $p_1^{t_1} ... p_s^{t_s} = r \in S$.

The following result involves our definitions of ideal components, decomposition fields, and generating functions in $\mathbb{Z}[G]$ associated to a difference set; for a difference set D, the *generating function* is simply the function $D(x) \in \mathbb{Z}[G]$ defined earlier. In what follows, we refer to this function as $g(x)$ rather than $D(x)$, retaining the convention in Yamamoto's paper. Since we work modulo $1 - x^v$, $x^{-1} = x^{v-1}$. Thus, in Yamamoto's notation, an equality we

stated earlier is rewritten as

$$g(x)g(x^{v-1}) \equiv n + \lambda(1 + x + ... + x^{v-1}) \pmod{1 - x^v}.$$

This implies in particular that if ω is a vth root of unity not equal to 1, then $g(\omega)g(\overline{\omega}) = n$. We now proceed to Yamamoto's second theorem.

Theorem 5.3 (Yamamoto, Thm. 2)**.** *Suppose that there exists a (v, k, λ)-difference set D. Let $p \mid n$ be a prime and $d \mid v$ be not equal to 1. Suppose further that $(p, d) = 1$ and that the decomposition field K_p of p is real, i.e., $K \subset \mathbb{R}$. Then the exponent of the p-component of n is even.*

Proof. Denote the complex conjugation automorphism by τ. Then $\tau \in \mathrm{Gal}(\mathbb{Q}(\omega_d)/\mathbb{Q})$. Moreover, $\tau \in D_p$, as K_p is real. In particular, $g(\omega_d)$ and $\tau(g(\omega_d))$ have the same $\mathfrak{p}$-component for any prime ideal $\mathfrak{p}$ dividing (p). Thus they must have the same p-component. Denote this p-component by $\mathfrak{b}$. Since $d \neq 1$, we have

$$g(\omega_d)g(\tau(\omega_d)) = n.$$

Write the p-component of n as p^e. Then it follows from the centered equality above that

$$p^e = \mathfrak{b}\tau(\mathfrak{b}) = \mathfrak{b}^2.$$

In particular, all prime ideal divisors $\mathfrak{p}$ of (p) divide $\mathfrak{b}$ with the same exponent. But by our Lemma 4.29, p is unramified in $\mathbb{Q}(\omega_d)$. Therefore, $\mathfrak{b}$ must be a power of (p), and we conclude that the exponent e of p^e is even. □

We state the following two corollaries without proof.

Corollary 5.4. *Suppose there exists a (v, k, λ)-difference set D with real decomposition field Δ. Then $n = k - \lambda$ is a square.*

Corollary 5.5. *Suppose there exists a (v, k, λ)-difference set. Let q be odd, and define $q^* := (-1)^{(q-1)/2}q$. If p is a prime, p^e is the p-compoennt of $n = k-\lambda$, and $q \mid v$ is odd, then*

$$(p^e, q^*)_r = 1$$

for all primes r (not including the infinite prime). That is to say, there then exists a non-zero solution to the following equation in $\mathbb{Q}_r$:

$$p^e x^2 + (-1)^{(q-1)/2} q y^2 = z^2.$$

Although this theorem gives a Diophantine equation the existence of solution to which depends on the existence of a (v, k, λ)-difference set, it is not so useful to apply because the solutions possibly exist in some p-adic field. However, it paves the road for subsequent theorems from Yamamoto's paper, which will use it in their proofs. We now state Yamamoto's third theorem, which is much easier to apply.

Theorem 5.6 (Yamamoto, Thm. 3)**.** *(i) Retain the notation of Yamamoto's second theorem. Additionally, let p^e and p^ℓ be the p-components of n and v, respectively. Then $p^{e/2} \leq (v/d)p^{-\ell}$.*

(ii) Suppose there exists a difference set with parameters (v, k, λ). Let $p \mid n = k-\lambda$ be prime, and let p^e and p^ℓ be defined as in part (i). If e is even, then $p^{e/2} \leq vp^{-\ell}$.

Proof. Let D be our (v, k, λ)-difference set. Set $w := dp^\ell$ in (i) and $w := p^\ell$ in (ii). As earlier, write $g(x)$ for the generating function of D, which is an element of $\mathbb{Z}[G]$, where G

is the ambient group containing D. By the proof of Theorem 2 of Yamamoto's paper, the decomposition group D_p contains the complex conjugation automorphism τ. In particular, any prime ideal $\mathfrak{p}$ dividing (p) is invariant under τ, and the p-component $\mathfrak{b}$ of $g(\omega_w)$ satisfies $(p^e) = \mathfrak{b}^2$. So by Theorem 2, e is even under the assumptions of (i), and it is also assumed to be even in (ii). Therefore, in either case we have $g(\omega_w) \equiv 0 \pmod{p^{e/2}}$. Indeed, $g(\omega) = 0 \pmod{p^{e/2}}$ for any wth root of unity $\omega \neq 1$.

Let us now deal with the $\omega = 1$ case. We have $g(1) = k$, which may not be divisible by $p^{e/2}$. But then either $k(v-k) \equiv 0 \pmod{p^e}$ (because the equality $k(k-1) = \lambda(v-1)$ is equivalent to $k(v-k) = n(v-1)$) or at least one of the numbers $g(1) = k$ and $g_{\overline{D}}(1) = v-k$ is congruent to 0 modulo $p^{e/2}$; here $g_{\overline{D}}$ is the generating function of the complement $\overline{D} = G \setminus D$, which is a difference set as well as is not difficult to show. Thus, possibly replacing D by $\overline{D}$, we may assume that $g(\omega) \equiv 0 \pmod{p^{e/2}}$ for any wth root of unity ω.

Let $g_w(x) := \sum_{i=0}^{w-1} C(i)x^i$, where $C(i) := |\{d \in D | d \equiv i \pmod{w}\}|$. Then $g_w(\omega) = g(\omega) \equiv 0 \pmod{p^{e/2}}$ for any wth root of unity ω, so we can apply Yamamoto's first theorem. We then obtain that, in the case of (i), if $d = q_1^{t_1}...q_r^{t_r}$ for primes $q_1, ..., q_r$, then

$$q_1^{t_1}...q_r^{t_r}\Delta(wq_1^{-t_1-1}...\Delta(wq_r^{-t_r-1})\Delta(wp^{-1})C(i) \equiv 0 \pmod{p^{e/2}}.$$

Since $(d, p) = 1$ and $\Delta(wq_j^{-t_j-1})$ for $j = 1, ..., r$ all act as the identity, $\Delta(wp^{-1})C(i) \equiv 0 \pmod{p^{e/2}}$ for all i. In the case of (ii), on the other hand, this congruence is an immediate result of Yamamoto's first theorem.

Now, suppose $\Delta(wp^{-1})C(i) = 0$ for all i. Then

$$\Delta(wq_1^{-1})...\Delta(wq_r^{-1})\Delta(wp^{-1})C(i) = 0$$

for all i, so taking $\alpha = 0$ in Yamamoto's first theorem gives $g_w(\omega_w) = g(\omega_w) = 0$. Because $g(\omega)g(\tau(\omega)) = n$, this gives $n = 0$, which is a contradiction. A similar argument holds in the case of (ii). It follows that there is an i for which $\Delta(wp^{-1})C(i) \neq 0$. We thus know that $C(i + wp^{-1}) - C(i) \equiv 0 \pmod{p^{e/2}}$ but that $C(i + wp^{-1}) - C(i) \neq 0$ for some i. As $C(i) = |\{d \in D | d \equiv i \pmod{w}\}$, $0 \leq C(i) \leq \frac{v}{w}$ for all i, as D is a difference set. For the choice of i that makes $C(i + wp^{-1}) - C(i)$ non-zero, we thus have

$$p^{e/2} \leq |C(i + wp^{-1}) - C(i)| \leq \frac{v}{w} = \frac{v}{d}p^{-\ell}.$$

This proves case (i), and taking $d = 1$ gives case (ii) as well. □

We have the following corollary.

Corollary 5.7. *The decomposition field of a non-trivial difference set is not real, i.e., it is not a subset of* $\mathbb{R}$.

Yamamoto notes at this point that there were 12 choices of (v, k, λ) with $3 \leq k \leq 50$ and $k < v/2$ for which the non-existence of corresponding difference sets had not been proved at the time of writing (1963). All of these can be proved not to exist with Yamamoto's third theorem alone.

The corollary to Yamamoto's third theorem suggests that it is worthwhile to consider difference sets other than those with real decomposition fields. Yamamoto's fourth theorem is

therefore a more general statement with no explicit restriction on the type of decomposition field. Indeed, it can be applied to the case of difference sets with imaginary quadratic difference fields.

Theorem 5.8 (Yamamoto, Thm. 4)**.** *Let q be a prime divisor of v such that $q \equiv -1 \pmod 4$ and let q^ℓ be the q-component of v. Assume that any prime divisor p of $n = k - \lambda$ satisfies (i) $ord_q p \equiv 0 \pmod 2$, (ii) $ord_{q^\ell} p = \frac{1}{2}q^{\ell-1}(q-1)$, or (iii) $p = q$. If there exists a (v, k, λ)-difference set D, then the Diophantine equation*

$$4n = x^2 + qy^2, 0 \le x, 0 \le y \le \frac{v}{q^\ell}, x + y \le \frac{2v}{q^\ell}$$

has a solution.

Proof. Let $\mathrm{Gal}(\mathbb{Q}(\omega_{q^\ell})/\mathbb{Q}) = \langle\sigma\rangle$, let $g(x)$ be the generating function corresponding to D, and let $\mathfrak{b}_p$ be the p-component of $g(\omega_{q^\ell})$. Suppose (i) holds, i.e., $\mathrm{ord}_q(p)$ is even. It follows by Theorem 2 that $\mathfrak{b}_p = (p)^e$ for some $e \in \mathbb{N}$.

Now suppose (ii) holds, i.e., $\mathrm{ord}_{q^\ell}(p) = \frac{1}{2}q^{\ell-1}(q-1)$. Then,

$$(p) = \mathfrak{p}\overline{\mathfrak{p}}$$

for a prime ideal $\mathfrak{p}$, and moreover $D_p = \langle\sigma^2\rangle$. Therefore, $\sigma^2(\mathfrak{p}) = \mathfrak{p}$ and $\sigma^2(\overline{\mathfrak{p}}) = \overline{\mathfrak{p}}$. The last statement holds also in case (iii).

In any case, we have $\sigma^2(\mathfrak{b}_p) = \mathfrak{b}_p$ for all prime divisors p of n. In particular, setting $\gamma := g(\omega_{q^\ell})$ gives $\sigma^2(\gamma) = (\gamma)$. Setting $\eta := \gamma^{1-\sigma^2} (:= (1-\sigma^2)(\gamma))$, we have that η is a unit of $\mathbb{Q}(\omega_{q^\ell})$. Also, letting τ denote complex conjugation,

$$\begin{aligned}\eta^{1+\tau} &= \gamma^{(1-\sigma^2)(1+\tau)} \\ &= \gamma^{(1+\tau)(1-\sigma^2)} \\ &= n^{1-\sigma^2} \\ &= 1,\end{aligned}$$

so $|\eta| = 1$. Since $\eta \in \mathbb{Q}(\omega_{q^\ell})$, η is a root of unity. Thus we can write $\eta = \epsilon\omega_{q^\ell}^j$ for $\epsilon = \pm 1$ and some j.

We claim that $\epsilon = 1$. Indeed, setting $N := q^{\ell-1}(q-1)$, we have

$$\begin{aligned}1 &= \eta^{1+\sigma^2+\ldots+\sigma^{N-2}} \\ &= \epsilon^{N/2}\sigma_{q^\ell}^{j(1+\sigma^2+\ldots+\sigma^{N-2})},\end{aligned}$$

from which it follows that $\epsilon = 1$ since $N/2$ is odd. Also, if $\omega_{q^\ell}^\sigma = \omega_{q^\ell}^s$ for some integer s, then the above shows that $j(1-s^N)/(1-s^2) \equiv 0 \pmod{q^\ell}$. Therefore, there exists u such that $-j \equiv (1-s^2)u \pmod{q^\ell}$. Since $1 - s^2 \not\equiv 0 \pmod q$ if $q \neq 3$ and since if $q = 3$, then the 3-components of $1 - s^2$ and $1 - s^N$ are 3 and 3^ℓ, respectively, we have that $j \equiv 0 \pmod 3$ and that there exists u such that $-j \equiv (1-s^2)u \pmod{3^\ell}$.

If necessary, we replace D with $D + u$. Then η becomes

$$(\omega_{q^\ell}^u g(\omega_{q^\ell})^{1-\sigma^2} = \omega_{q^\ell}^{u(1-\sigma^2)}\eta$$

$$= \omega_{q^\ell}^{(1-s^2)u+j}$$
$$= 1.$$

So by replacing D with $D+u$, we may assume that $g(\omega_{q^\ell})^{\sigma^2} = g(\omega_{q^\ell})$. We then have that $\gamma := g(\omega_{q^\ell})$ is an element of the ring of integers of $\mathbb{Q}(\sqrt{-q})$; notice that $n = \gamma^{1+\tau}$ is the norm of γ. In particular, we can write $\gamma = a + b\zeta$ where $\zeta := (-1+\sqrt{-q})/2$. Then $4n = (2a-b)^2+qb^2$. Letting g_{-D} denote the generating function of $-D$ and $g_{\overline{D}}$ the generating function of the complement of D, we have

$$g_{\overline{D}}(\omega_{q^\ell}) = -a - b\zeta,$$
$$g_{-D}(\omega_{q^\ell}) = a + b\zeta^\tau = a - b - b\zeta,$$
$$g_{-\overline{D}}(\omega_{q^\ell}) = -a + b + b\zeta,$$

so we can assume $a \geq 0$ and $b \geq 0$ by replacing D with $-D, \overline{D}$, or $-\overline{D}$ if necessary. From classical analytic number theory, we know we can rewrite ζ as a Gauss sum

$$\zeta = \sum_{i=1}^{q-1} \psi(i)\omega_q^i = \pm \sum_{i=1}^{q-1} \psi(i)\omega_{q^\ell}^{q^{\ell-1}i},$$

where $\psi(i) = 0$ or 1 depending on whether i is a quadratic non-residue or residue modulo q, respectively. Also, ω_q is a suitable primitive qth root of unity, and the sign $\pm$ is the sign of (j/q) for j such that $\omega_{q^\ell}^{q^{\ell-1}} = \omega_q^j$. Letting

$$g_{q^\ell}(x) = \sum_{i=0}^{q^\ell-1} C(i)x^i,$$

where the $C(i)$ are defined as earlier in this article, we have that

$$g_{q^\ell}(x) - (a \pm b\sum_{i=1}^{q-1} \psi(i)x^{q^{\ell-1}i}$$

has a zero at $x = \omega_{q^\ell}$, so by applying Yamamoto's first theorem with $\alpha = 0$, we get

$$C(0) - a = C(q^{\ell-1}i) \mp b\psi(i)$$

for $i = 1, 2, ..., q-1$. In particular, $C(0) - a = C(q^{\ell-1}) \mp b = C(-q^{\ell-1})$. As $0 \leq C(i) \leq v/q$ for all i, we obtain $a \leq vq^{-\ell}$ and $b \leq vq^{-\ell}$. Similarly, using $g_{-\overline{D}}(\omega_{q^\ell}) = -a + b + b\zeta$ instead gives $|a-b| \leq vq^{-\ell}$. Taking $x := |2a-b|, y := b$ now yields the result. □

We have the following corollary to Yamamoto's fourth theorem.

Corollary 5.9. *Consider a hypothetical (v,k,λ)-difference set. Let $v = q^\ell$, where q is a prime $\equiv 3 \pmod 4$. Suppose some prime divisor p of $n = k - \lambda$ has even order or the order of $\frac{1}{2}(q-1) \pmod q$, $p^{q-1} \not\equiv 1 \pmod{q^2}$. Then our hypothetical difference set exists only if $\ell = 1$ and $q > 3$. In this case, we obtain exactly two difference sets, with parameters $v = q$ and $n = \frac{1}{4}(q+1)$.*

Yamamoto's fifth and sixth theorems are quite similar to the fourth theorem in that they concern difference sets with no explicit restriction on the type of decomposition field they have.

Theorem 5.10 (Yamamoto, Thm. 5)**.** *Let q and r be distinct prime divisors of v, let q^ℓ and r^m be the q-components and r-components of v, respectively, and let $q \equiv -1 \pmod 4$,*

$(\varphi(q^\ell), \varphi(r^m)) = 2$, where φ is the Euler totient function. Assume that any prime divisor of n satisfies one of the following:
(i) $ord_q p \equiv 0 \pmod 2$ and $ord_r p \equiv 0 \pmod 2, \not\equiv 0 \pmod 4$,
(ii) $ord_{q^\ell} p = \frac{1}{2}\varphi(q^\ell)$ and $ord_{r^m} p = \varphi(r^m)$,
(iii) $p = q$ and $ord_{r^m} p = \varphi(r^m)$.

If there exists a (v, k, λ)-difference set D, then there is a solution to the Diophantine equation

$$4n = x^2 + qy^2, 0 \le x, 0 \le y \le \frac{2v}{q^\ell r^m}, x + y \le \frac{4v}{q^\ell r^m}.$$

Proof. Let $g(x)$ be the generating function of D and set $w := q^\ell r^m$. We then observe that $\mathbb{Q}(\omega_m)$ is the compositum of $\mathbb{Q}(\omega_{q^\ell})$ and $\mathbb{Q}(\omega_{r^m})$, i.e., the smallest field extension of $\mathbb{Q}$ containing both. Also, if $\mathrm{Gal}(\mathbb{Q}(\omega_{q^\ell})/\mathbb{Q}) = \langle\sigma\rangle$ where σ acts as the identity on $\mathbb{Q}(r^m)$, and if $\mathrm{Gal}(\mathbb{Q}(\omega_{r^m})/\mathbb{Q}) = \langle\rho\rangle$ where ρ acts as the identity on $\mathbb{Q}(\omega_{q^\ell})$, then $\mathrm{Gal}(\mathbb{Q}(\omega_w)/\mathbb{Q}) = \langle\sigma, \rho\rangle$.

Suppose p satisfies condition (i). Then there exists z such that $p^z \equiv -1 \pmod w$ and, letting $\mathfrak{b}_p$ denote the p-component of $g(\omega_w)$, $\mathfrak{b}_p$ is rational by Yamamoto's second theorem.

If p satisfies (ii), then $\mathrm{ord}_w(p)$ is the least common multiple of $\mathrm{ord}_{q^\ell}(p)$ and $\mathrm{ord}_{r^m}(p)$, which is $\frac{1}{2}\varphi(w)$ by the assumptions of the theorem. We observe that the decomposition field of p is $\mathbb{Q}(\sqrt{-q})$, so any prime ideal divisor $\mathfrak{p}$ of (p) originates in $\mathbb{Q}(\sqrt{-q})$.

If p satisfies (iii), then $p = q = \mathfrak{q}^{\varphi(q^\ell)}$, where $\mathfrak{q}$ is the prime ideal divisor of (q). Since the q-component $\mathfrak{b}_q$ of $g(\omega_w)$ is a power of $\mathfrak{q}$, it is rational, and Yamamoto's second theorem gives us that the q-component of n must be a square. Setting $\gamma := g(\omega_w)$, $\eta := \gamma^{1-\sigma^2}$, $\theta := \omega^{1-\rho}$, we see that η and θ are units in $\mathbb{Q}(\omega_w)$. Thus $\eta^{1+\tau} = \theta^{1+\tau} = 1$, and we can show, as in the proof of Yamamoto's fourth theorem, that η and τ are roots of unity in $\mathbb{Q}(\omega_w)$. In particular, $\eta^{1-\rho}$ is a q^ℓth root of unity and $\theta^{1-\sigma^2}$ is an r^mth root of unity. However, both of these are equal to $\gamma^{(1-\sigma^2)(1-\rho)}$, so we see that $\eta^{1-\rho} = \theta^{1-\sigma^2} = 1$, and thus that η is a root of unity of $\mathbb{Q}(\omega_{q^\ell})$ and θ is a root of unity in the subfield K fixed by σ^2.

One can show that K is the compositum of $\mathbb{Q}(\omega_{r^m})$ and $\mathbb{Q}(\sqrt{-q})$ of degree $2\varphi(r^m)$ over $\mathbb{Q}$., and unless $q = 3$, θ is a root of unity in $\mathbb{Q}(\omega_{r^m})$. On the other hand, if $q = 3$, θ may be a $6r^m$th root of unity. We obtain as in the proof of Yamamoto's fourth theorem that $\eta = \epsilon\omega_{q^\ell}^i, \theta = \epsilon'\omega_{r^m}^q$ (for $q \ne 3$) or $\theta = \epsilon'\omega_{r^m}^j\omega_3^a$ (for $q = 3$), where i, j, a are integers and $\epsilon, \epsilon' = \pm 1$. As in the proof of Yamamoto's fourth theorem, we then find that $\epsilon = 1$ and that by replacing D by $D + ur^m$ for some u if needed, we can assume $\eta = 1$. Similarly, replacing D by $D + u'q^\ell$ for some u' if needed, we can assume that $\theta = \epsilon'$ (if $q \ne 3$) or that $\theta = \epsilon'\omega_3^a$ (if $q = 3$).

First, let us consider the $q \ne 3$ case. We claim that $\epsilon' = 1$. Since $\gamma^{1-\sigma^2} = 1$ and $\gamma^{1-\rho} = \epsilon' = \pm 1$, we have that $\gamma^2 \in \mathbb{Q}(\sqrt{-q})$. Setting $\mathfrak{D} := \mathbb{Z}[\omega_w]$ and $\mathfrak{v} := \mathbb{Z}[\zeta]$ where $\zeta = (-1 + \sqrt{-q})/2$, we have $\gamma\mathfrak{D} = \mathfrak{c}\mathfrak{D}$ for some ideal $\mathfrak{c}$ of $\mathfrak{v}$, as $\gamma\mathfrak{D}$ originates in $\mathbb{Q}(\sqrt{-q})$. However, we also have $\gamma^2 \in \mathfrak{v}$, so $\mathfrak{c}^2 = \gamma^2\mathfrak{v}$ is a principal ideal of $\mathfrak{v}$, and therefore $\mathfrak{c}$ itself must be principal, from the theory of imaginary quadratic fields (in particular, the fact that

$\mathbb{Q}(\sqrt{-q})$ has odd class number, as it has prime discriminant).

If $\mathfrak{c} = \gamma_0\mathfrak{v}$ for some $\gamma_0 \in \mathfrak{v}$, then $\gamma^2 = \gamma_0^2\eta_0$ for some unit η_0 of $\mathbb{Q}(\sqrt{-q})$. But then we have $\eta_0 = \pm 1$. If $\eta_0 = -1$, then $\gamma\gamma_0^{-1} = \sqrt{-1} \in \mathbb{Q}(\omega_w)$, a contradiction. So $\eta_0 = 1$ and $\gamma = \pm\gamma_0 \in \mathbb{Q}(\sqrt{-q})$.

Now let us deal with the case where $q = 3$. Then $\gamma^{2(1-\sigma^2)} = 1$ and $\gamma^{2(1-\rho)} = \omega_3^{2a}$ for suitable a. We claim that $a \equiv 0 \pmod 3$. Suppose otherwise. Then γ^2 determines a degree 3 subfield K over $\mathbb{Q}(\sqrt{-q})$, which is only possible if $r \equiv 1 \pmod 3$. It is also the case that K is uniquely determined as the subfield of $\mathbb{Q}(\omega_w)/\mathbb{Q}(\omega_3)$ of degree 3 relative to $\mathbb{Q}(\omega_3)$. Setting

$$\xi := \sum_{i=0}^{(1/3)(r-1)-1} \omega_r^{\rho^{3i}},$$

we observe that ξ, ξ^ρ, and ξ^{ρ^2} determine a basis for K with respect to $\mathbb{Z}[\omega_3]$. Then $(\gamma^2)^{1-\rho} = \gamma_3^{-a}$ tells us that

$$\begin{aligned}\gamma^2 &= \alpha_0(\xi + \omega_3^a\xi^\sigma + \omega_3^{2a}\xi^{\sigma^2}) \\ &= \alpha_)A\end{aligned}$$

for some $\alpha_0 \in \mathbb{Z}[\omega_3]$. Letting $\Lambda := \xi + \omega_3^a\xi^\sigma + \omega_3^{2a}\xi^{\sigma^2}$, we have $\Lambda^{1+\tau} = r$. Therefore, we obtain $n^2 = \gamma^{2(1+\tau)} = \alpha_0^{1+\tau}r$. But $(n, r) = 1$ by assumption, so we reach a contradiction.

We know that $\gamma^2 \in \mathbb{Q}(\sqrt{-3})$ and wish to prove that $\gamma \in \mathbb{Q}(\sqrt{-3})$. Setting $\mathfrak{v} := \mathbb{Z}[\omega_3], \mathfrak{D} := \mathbb{Z}[\omega_w]$, we know that $\gamma\mathfrak{D} = \mathfrak{c}\mathfrak{D}$ for some ideal $\mathfrak{c}$ of $\mathfrak{v}$, as in the earlier case. Once again, as $\mathbb{Q}(\sqrt{-3})$ has class number 1, we know that $\mathfrak{c}$ must be a principal ideal, so that $\gamma\mathfrak{D} = \gamma_0\mathfrak{D}$ for some $\gamma_0 \in \mathfrak{v}$. However, $\gamma^2 \in \mathfrak{v}$ and $\gamma^2 = \gamma_0^2\eta_0$ for some unit η_0 of $\mathfrak{v}$. We observe that η_0 is a 6th root of unity, and $\eta_0^{1/2} = \gamma\gamma_0^{-1}$ must be a root of unity in $\mathbb{Q}(\omega_w)$. Therefore, η_0 is a third root of unity. In particular, $\gamma = \eta_0^{1/2}\gamma_0 \in \mathbb{Q}(\sqrt{-3})$.

We know that $\gamma = g(\omega_w)$ is in the ring of integers of $\mathbb{Q}(\sqrt{-q})$. Let $\gamma = a + b\zeta$ with $\zeta = (-1 + \sqrt{-q})/2$. Setting $g_w(x) := \sum_{i=0}^{w-1} C(i)x^i$, the polynomial

$$g_w(x) - (a \pm b\sum_{i=1}^{q-1} \psi(i)x^{q^{\ell-1}r^m i}),$$

where $\psi(i) = \frac{1}{2}((i/q) + 1)$ ((i/q) is the Legendre symbol), has a root at $x = \omega_w$. Therefore, Yamamoto's first theorem tells us that

$$C(0) - a - C(q^{\ell-1}r^m i) \mp b\psi(i) = C(q^\ell r^{m-1}) - C(q^\ell r^{m-1}j + q^{\ell-1}r^m i)$$

for $i = 1, 2, ..., q-1$ and $j = 1, 2, ..., r-1$. As $0 \le C(i) \le v/w$, we have $|a| \le 2v/w$, $|b| \le 2v/w$, and $|a - b| \le 2v/w$, as in the proof of Yamamoto's fourth theorem. Therefore, $4n = 4\gamma^{1+\tau} = x^2 + qy^2$, where, choosing $x := |2a - b|, y := |b|$, $0 \le x$, $0 \le y \le 2v/w$, and $x + y \le 4v/w$. □

We have the following corollary.

Corollary 5.11. *Retain the notation of Yamamoto's fifth theorem and take $v = q^\ell r^m$. Then the only possibility is $v = 21, n = 4$.*

Finally, we prove the sixth and final paper of Yamamoto's paper. It is quite similar and structure to his fourth and fifth theorems.

Theorem 5.12 (Yamamoto, Thm. 6)**.** *Let q and r be prime divisors of v such that $q \equiv -1 \pmod 4, r \equiv 1 \pmod 4, (q/r) = -1$, and $(\varphi(q^\ell), \varphi(r^m)) = 2$ for q^ℓ and r^m the q- and r-components of v, respectively. Assume any prime divisor p of n satisfies either*

(i) $ord_q p \equiv 0 \pmod 2$ and $ord_r p \equiv 0 \pmod 2, \not\equiv 0 \pmod 4$, or

(ii) $ord_{q^\ell} p = \varphi(q^\ell)$ and $ord_{r^m} p = \varphi(r^m)$.

Then, if there exists a (v, k, λ)-difference set D, there is a solution to the Diophantine equation

$$4n = x^2 + qry^2, 0 \le x, 0 \le y \le \frac{2v}{q^\ell r^m}, x + y \le \frac{4v}{q^\ell r^m} - 2.$$

Proof. As earlier, we let $g(x)$ be the generating function of D. We also set $w := q^\ell r^m$. Let the p-component of $g(\omega_w)$ be $\mathfrak{b}_p$. Then $\mathfrak{b}_p$ is rational for p satisfying condition (i), by an application of Yamamoto's second theorem. Also, if p satisfies condition (ii), then by assumption the decomposition field $K_p = \mathbb{Q}(\sqrt{-qr})$.

Now, let $\mathrm{Gal}(\mathbb{Q}(\omega_{q^\ell})/\mathbb{Q}) = \langle\sigma\rangle$ and $\mathrm{Gal}(\mathbb{Q}(\omega_{r^m})/\mathbb{Q}) = \langle\rho\rangle$, where σ and ρ act as the identity on $\mathbb{Q}(\omega_{r^m})$ and $\mathbb{Q}(\omega_{q^\ell})$, respectively. Then $\mathrm{Gal}(\mathbb{Q}(\omega_w)/\mathbb{Q}) = \langle\sigma, \rho\rangle$. Setting $\gamma := g(\omega_w)$, we have that $\eta := \gamma^{1-\sigma\rho}$ has $\eta^{1+\tau} = 1$, so is a root of unity.Replacing D by $D + uq^\ell + u'r^m$ if needed, we can assume $\eta = \pm 1$. Just as in the proofs of Yamamoto's fourth and fifth theorems, $\gamma^{1-\sigma^2} = \gamma^{1-\rho^2} = 1$ Therefore, γ^2 is an element of the subfield of $\mathbb{Q}(\omega_w)$ that is fixed by σ^2, ρ^2, and $\sigma\rho$. This subfield is $\mathbb{Q}(\sqrt{-qr})$.

We claim, as in the proof of Yamamoto's fifth theorem, that $\gamma \in \mathbb{Q}(\sqrt{-qr})$. Suppose it does not. Then $\gamma^{1-\sigma\rho} = -1$ and $\gamma = \frac{1}{2}(c\sqrt{-q} + d\sqrt{r})$ for some $c, d \in \mathbb{Z}$ such that $c \equiv d \pmod 2$. Then we have $4n = 4\gamma^{1+\tau} = qc^2 + rd^2$. But this cannot hold, as n is a square and we assumed that $(q/r) = -1$. Therefore, $\gamma \in \mathbb{Q}(\sqrt{-qr})$, so $\gamma = a + b\zeta$ for some a, b, where $\zeta = (-1 + \sqrt{-qr})/2$. Note that by the theory of Gauss sums, if $\psi(i) := \frac{1}{2}((i/(qr) + 1)$, where (i/qr) is the Jacobi symbol, then

$$\zeta = \sum_{i=1}^{qr-1} \psi(i)\omega_{qr}^i,$$

where ω_{qr} is a suitable primitive qrth root of unity. Letting $g_w(x) := \sum_{i=0}^{w-1} C(i)x^i$, we observe that the polynomial

$$g_w(x) - (a \pm b \sum_{i=1}^{qr-1} \psi(i) x^{q^{\ell-1}r^{m-1}i})$$

has a root at $x = \omega_w$. Applying Yamamoto's first theorem with $\alpha = 0$ gives

$$C(0) - a - (C(q^{\ell-1}r^m i) - \frac{1}{2})$$

$$= C(q^\ell r^{m-1} j) - \frac{1}{2} - (C(q^{\ell-1}r^m i + q^\ell r^m j) \mp b\psi(ri + qj)).$$

We can rephrase this as

$$C(0) - a + 1 - C(q^{\ell-1}r^m i) = C(q^\ell r^{m-1} j) - C(q^{\ell-1}r^m i + q^\ell r^{m-1} j) \mp b\psi(ri + qj)$$

for $i = 1, 2, ..., q-1$ and $j = 1, 2, ..., r-1$. Since $0 \leq C(i) \leq v/w$ or all i, we obtain $|a-1| \leq 2v/w$, $|b| \leq 2v/w$. Considering $\overline{D}$ instead of D if necessary, we also have $|-a-1| \leq 2v/w$, i.e., $|a| \leq 2v/w - 1$. Likewise considering $-D$ instead of D, we obtain $|a-b| \leq 2v/w - 1$. Taking $x := |2a-b|, y := |b|$, we obtain

$$4n = 4\gamma^{1+\tau} = x^2 + qy^2,$$
$$0 \leq x, 0 \leq y \leq 2v/w, x + y \leq 4v/w - 2.$$

This proves the result. □

6. Applications

Now that we have completed our journey through Yamamoto's paper, the reader may be curious what the payoff is. Indeed, it is customary, when one has written a paper about difference sets, to numerically check how many difference sets in a given range of parameters can be proved to not exist using the methods in one's paper. Yamamoto carried out this calculation. He found 373 choices of v and n with $2 \leq n \leq 50$ and satisfying the elementary condition $k(v-k) = n(v-1)$. In 273 of these cases, he was able to use his second, third, fourth, fifth, and sixth theorems to establish non-existence. Of the remaining 100 cases, 58 parameters were already known to correspond to existent difference sets, so they would have been impossible to rule out by any method. The remaining 42 cases involved difference sets with decomposition fields of degree higher than 2, and the theorems in Yamamoto's paper were not able to rule out their existence.

References

[1] E.H. Moore and H.S. Pollatsek. *Difference Sets: Connecting Algebra, Combinatorics, and Geometry.* American Mathematical Society. (2013).

[2] S. Alaca and K.S. Williams. *Introductory Algebraic Number Theory.* Cambridge University Press. (2004).

[3] K.W. Smith. *Non-abelian Hadamard Difference Sets.* J. Combin. Theory A 70, 144–145. (1995).

[4] J.M. Masley. *Solution of the class number two problem for cyclotomic fields.* Inventiones 28, 234–244. (1975).

[5] H.M. Edwards. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* Springer. (2000).

[6] J. Neukirch (transl. Norbert Schappacher). *Algebraic Number Theory.* Springer–Verlag. (1999).

[7] J.E. Iiams. *On difference sets in groups of order $4p^2$.* J. Combin. Theory A 72, 256–276. (1995).

[8] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory (2nd Ed.).* Cambridge University Press, 2 vol. (1999).

[9] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory (2nd Ed.).* Springer–Verlag. (1982).

[10] K. Yamamoto. *Decomposition Fields of Difference Sets.* Pacific Journal of Mathematics, Vol. 13, No. 1. (1963).